ABSTRACT OF THE DISCLOSURE

Techniques for securing data in communications between a client and server using an unencrypted transfer protocol, which does not encrypt a payload defined by the transfer protocol, include selecting a subset from a set of data to be communicated in a particular payload. A secret integer is determined that is unique for the subset. Based on the subset and the secret integer, encrypted data is generated that is practically unintelligible to a device other than the client and the server. A sending device, of the client and the server, sends to a receiving device, in the particular payload, the encrypted data and information to determine, only at the client and the server, the secret integer for decrypting the encrypted data. The present techniques allow a lightweight encryption algorithm to provide authentication and data security for more secure transfer of selective portions of unencrypted payloads transferred by such protocols as the Hypertext Transfer Protocol (HTTP).